PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY

of the

SENATE COMMITTEE ON THE JUDICIARY

on

Identity Theft: Innovative Solutions for an Evolving Problem

Washington, DC

March 21, 2007

I. INTRODUCTION

Madam Chairman, Senator Kyl, and members of the Subcommittee, I am Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the important and interrelated issues of identity theft; data security; and the collection, use, and disclosure of Social Security numbers ("SSNs").

Identity theft is a pernicious crime and controlling it is a critical component of the Commission's consumer protection mission. This testimony describes the nature and scope of the identity theft problem and the critical role that SSNs play both in creating and solving the problem. This testimony also will summarize the Commission's efforts to combat identity theft through its law enforcement actions against companies that failed to reasonably protect consumer data, its participation on the Identity Theft Task Force, and its extensive consumer and business education and outreach efforts.

II. THE IDENTITY THEFT PROBLEM

Identity theft has become a serious concern in our information-based economy. Millions of consumers are victimized by this crime every year.[2] Generally speaking, there are two varieties of identity theft: the takeover or misuse of existing credit card, debit card, or other accounts ("existing account fraud"); and the use of stolen information to open new accounts in

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any individual Commissioner.

[2] *See, e.g.,* http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf.

the consumer's name ("new account fraud"). New account fraud, although less prevalent, typically causes considerably more harm to consumers in out-of-pocket expenses and time necessary to repair the damage.[3]

Beyond its direct costs, concerns about identity theft harm our economy by threatening consumers' confidence in the marketplace generally, and in electronic commerce specifically. A recent Wall Street Journal/Harris Interactive survey, for example, found that, as a result of fears about protecting their identities, 30 percent of consumers polled were limiting their online purchases, and 24 percent were cutting back on their online banking.[4]

Identity theft has many causes, but this testimony will focus on two of them: the failure to protect consumers' sensitive personal information, which can lead to data breaches; and the availability of SSNs, with which identity thieves can open new accounts in consumers' names. The government and private sector must continue to work together to reduce the opportunities for thieves to obtain consumers' personal information, and make it more difficult for thieves to misuse the information if they do obtain it.

---

[3] Federal law limits consumers' liability for unauthorized credit card charges to $50 per card as long as the credit card company is notified within 60 days of the unauthorized charge. *See* 12 C.F.R. § 226.12(b). Many credit card companies do not require consumers to pay the $50 and will not hold consumers liable for the unauthorized charges, no matter how much time has elapsed since the discovery of the loss or theft of the card.

[4] *See* Jennifer Cummings, *Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft*, The Wall Street Journal Online, May 18, 2006, http://www.harrisinteractive.com/news/newsletters/WSJfinance/HI_WSJ_PersFinPoll_2006_vol2_iss05.pdf.

III. COMMISSION ACTIVITIES TO COMBAT IDENTITY THEFT

A. Law Enforcement on Data Security

One important way to keep sensitive information out of the hands of identity thieves is by ensuring that those who maintain such information adequately protect it. The Commission plays an active role in furthering this goal through law enforcement action against businesses that fail to implement reasonable security measures to protect sensitive consumer data.

Public awareness of, and concerns about, data security have reached new heights as reports about the latest data breaches of sensitive personal information continue to proliferate. Recent breaches have touched both the public and private sectors. Of course, not all data breaches lead to identity theft; in fact, many prove harmless or are caught and addressed before any harm occurs. Nonetheless, some breaches - especially those that result from deliberate actions, such as hacking, by criminals - have led to identity theft.

A number of bills have been introduced in the past two sessions of Congress that would require businesses that maintain sensitive consumer information to have reasonable protections in place to prevent unauthorized access, as well as to require companies that suffer a data breach to provide notice to affected consumers. Pending the enactment of broad data security legislation, the FTC enforces several laws that contain data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.[5] The Fair Credit Reporting Act

---

[5] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

("FCRA") includes certain due diligence requirements for consumer reporting agencies[6] and safe disposal obligations for companies that maintain consumer report information.[7] In addition, the FTC has enforced the Federal Trade Commission Act's proscription against unfair or deceptive acts or practices in cases where a business made false or misleading claims about its security procedures, or where its failure to employ reasonable security procedures caused substantial consumer injury.[8]

Since 2001, the Commission has brought fourteen cases challenging businesses that failed to reasonably protect sensitive consumer information that they maintained.[9] In a number of these cases, the Commission alleged that the company had misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive practices.[10] In addition, in several of the cases, the alleged security inadequacies led to breaches that caused

---

[6] 15 U.S.C. § 1681 et seq. The FCRA specifies that consumer reporting agencies may provide consumer reports only for enumerated "permissible purposes," and requires that they have reasonable procedures to verify the identity and permissible purposes of prospective recipients of their reports.

[7] The FTC's implementing disposal rule is at 16 C.F.R. Part 382.

[8] 15 U.S.C. § 45(a).

[9] *See generally* http://www.ftc.gov/privacy/index.html.

[10] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, FTC Matter No. 0623057 (Nov. 16, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (March 4, 2005); *In the Matter of MTS Inc., d/b/a/ Tower Records/Books/Video,* FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

substantial consumer injury and were challenged as unfair practices under the FTC Act.[11] Some of the cases involved enforcement of the Commission's GLB Act Safeguards Rule or the FCRA.[12]

Probably the best-known FTC data security case was its action against ChoicePoint, Inc. ChoicePoint, a data broker, inadvertently sold sensitive information (including credit reports in some instances) on more than 160,000 consumers to data thieves, who used that information in some cases to commit identity theft. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of its information. For example, the company allegedly approved as purchasers individuals who lied about their credentials, used commercial mail drops and business addresses, and faxed multiple applications from nearby commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for violations of the FCRA and $5 million in consumer redress for identity theft victims, and agreed to undertake substantial new data security measures.[13]

---

[11] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (March 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

[12] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group Inc.*, FTC Docket No. 9319 (April 15, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005). In the *Nations Title, Nationwide Mortgage Group,* and *Sunbelt Lending Services* cases, the Commission also alleged that the companies violated the GLB Act's privacy provisions and the FTC's implementing Privacy Rule, which, among other things, require financial institutions to provide notices to their customers describing their information-sharing policies.

[13] *See* FTC Press Release, *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.html. The Commission has mailed more than

The Commission's most recent data security enforcement action involved Guidance Software, Inc., a marketer of software and related services for investigating and responding to computer breaches and other security incidents. According to the FTC complaint, Guidance, in contrast to its claims, failed to implement simple, inexpensive and readily available security measures to protect consumers' data, for example, by permanently storing credit card information in clear, readable text rather than encrypting or otherwise protecting it.[14]

Although the Commission's data security cases have been brought under different laws, they share common elements: the vulnerabilities were multiple and systemic, and readily-available and often inexpensive measures were available to prevent them. Together, the cases stand for the proposition that companies should maintain reasonable and appropriate measures to protect sensitive consumer information.

The FTC Safeguards Rule promulgated under the GLB Act serves as a good model of this approach. Firms covered by the Rule must prepare a written plan; designate an official with responsibility for the plan; identify, assess, and address foreseeable risks; oversee their service providers handling of information; monitor and evaluate the program for effectiveness; and adjust the plan as appropriate. The Rule specifies that what is "reasonable" will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. This standard recognizes that there cannot be "perfect" security, and that data breaches can occur despite the maintenance of reasonable precautions to prevent them.

1,400 claims forms to possible victims and has created a website where consumers can download claims forms and obtain information about the claims process.

[14] *In the Matter of Guidance Software, Inc.*, FTC Matter No. 0623057 (Nov. 16, 2006).

It also is a flexible and adaptable standard that accounts for the fact that risks, technologies, and business models change over time, and that a static technology-based standard would quickly become obsolete and might stifle innovation in security practices. The Commission will continue to apply the "reasonable procedures" principles in enforcing existing data security laws.

B. Participation in the Identity Theft Task Force

On May 10, 2006, the President established an Identity Theft Task Force. Comprised of 18 federal agencies, the Task Force is chaired by Attorney General Alberto Gonzales and co-chaired by FTC Chairman Deborah Platt Majoras. The mission of the Task Force is to develop a comprehensive national strategy to combat identity theft.[15] The President specifically directed the Task Force to make recommendations on ways to improve further the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution.

On September 19, 2006, the Task Force published a set of interim recommendations on measures that could be implemented immediately to help address the problem of identity theft.[16] Broadly, these recommendations are organized around the principles of prevention (improving government handling of sensitive data and improving authentication methods), victim assistance, and law enforcement. These recommendations have been implemented or are in the process of being implemented.

---

[15] Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

[16] *See* FTC Press Release, *Identity Theft Task Force Announces Interim Recommendations* (Sept. 19, 2006), *available at* www.ftc.gov/opa/2006/09/idtheft.htm.

To supplement its research and analysis, on December 26, 2006, the Task Force solicited public comment on a list of possible additional recommendations.[17] The Task Force received approximately 150 comments, representing the views of trade associations, consumer advocacy groups, and identity theft victims. Many comments concerned the use of SSNs, their value in matching consumers to their information, and possible alternative identifiers. In addition, the Task Force received many comments stressing the need to enhance the prosecution of identity theft and to promulgate national standards for data security. The Task Force is in the process of reviewing the comments and preparing a final strategic plan and recommendations.

C. Consumer and Business Education

The Commission has undertaken substantial efforts to increase consumer and business awareness of the importance of protecting data and taking other steps to prevent identity theft. The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. The Commission receives about 15,000 to 20,000 contacts each week on how to recover from identity theft, or how to avoid becoming a victim in the first place. Callers to our hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft. The FTC's identity theft primer[18] and victim recovery guide[19] are widely available in print

---

[17] *See* FTC Press Release, *Identity Theft Task Force Seeks Public Comment* (Dec. 26, 2006), *available at* http://www.ftc.gov/opa/2006/12/fyi0688.htm.

[18] *Avoid ID Theft: Deter, Detect, Defend, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.

[19] *Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm.

and online. The Commission has distributed over 2 million copies of the primer and has recorded over 2.4 million visits to the Web version.

Last year, the Commission launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend." It includes direct-to-consumer brochures, as well as training kits and ready-made materials (including presentation slides and a video) for use by businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. The Commission has distributed over 1.5 million brochures and 40,000 kits to date. The Commission also has partnered with other organizations to broaden its reach. As just one example, the U.S. Postal Inspection Service recently initiated an outreach campaign to place FTC educational materials on subway cars in New York, Chicago, San Francisco, and Washington D.C.

The Commission also sponsors a multimedia website, OnGuard Online,[20] designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudsters. OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch has attracted more than 3.5 million visits.

The Commission directs its outreach to businesses as well. Just this month, the FTC released a new business education guide related to security.[21] Most companies have some information in their files - names, Social Security numbers, credit card numbers - that identifies

---

[20] *See* http://www.onguardonline.gov/index.html.

[21] *Protecting Personal Information: A Guide for Business, available at* http://www.ftc.gov/infosecurity.htm. Other business publications on data security and responding to data breaches are available at http://www.ftc.gov/bcp/edu/microsites/idtheft.htm.

their customers and employees. The Commission has heard from some businesses, particularly smaller businesses, that they were not sure what data security measures they should take to protect such sensitive information from falling into the wrong hands. FTC staff therefore developed a brochure that articulates the key steps that are part of a sound data security plan. The Commission anticipates that the brochure will prove to be a useful tool in alerting businesses to the importance of data security issues and give them a solid foundation on how to address those issues.

IV. PROTECTING AGAINST MISUSE OF SOCIAL SECURITY NUMBERS

Data breaches involving SSNs can be particularly harmful to consumers, because the SSN in many cases is the key piece of information that can enable criminals to perpetrate new account fraud. Making SSNs more difficult to obtain by criminals - and more difficult to use - is critical in the fight against this kind of identity theft.

A. The Uses and Sources of SSNs

SSNs play a vital role in our economy, enabling businesses, government, and others to match information to the proper individual. For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file, and that they are providing the right credit report for the right consumer. SSNs also are used in locator databases to find lost beneficiaries, witnesses, and law violators and to collect child support and other judgments. Employers must collect SSNs for tax reporting purposes, and health care providers may need them to facilitate Medicare reimbursement.

SSNs are available from both public and private sources. Public records in city and county offices across the country, including birth and death records and voter registrations, often

contain individuals' SSNs. There also are a number of private sources of SSNs, including consumer reporting agencies that include the SSN as part of the "credit header" information on consumer reports. Information brokers also collect personal information, including SSNs, from a variety of sources and compile and resell that data to third parties.

B. Current Laws Restricting the Use or Disclosure of SSNs

There are several federal and state laws and regulations that restrict the use or disclosure of SSNs in certain contexts.[22] Of most relevance is the GLB Act and its implementing regulations ("Privacy Rule"), which prohibit financial institutions from disclosing nonpublic personal information, including SSNs, to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.[23] The GLB Act and Privacy Rule include a number of exceptions under which disclosure is permitted without having to provide notice and opt out, including for purposes of credit reporting, fraud prevention, law enforcement, and compliance with judicial process.[24] Entities that receive nonpublic personal information under one of these exceptions are subject to the reuse and redisclosure restrictions of the Privacy Rule, even if those entities are not themselves financial institutions. More specifically, recipients may use or disclose the information only "in the ordinary course of

---

[22] For example, the FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003, requires consumer reporting agencies, upon the consumer's request, to truncate the SSN on reports provided to consumers. 15 U.S.C. § 1681g(a)(1)(A). The Driver's Privacy Protection Act prohibits state motor vehicle departments from disclosing personal information, including SSNs, in motor vehicle records, subject to several exceptions. 18 U.S.C. §§ 2721-25.

[23] 16 C.F.R. Part 313, implementing 15 U.S.C. § 6801 *et seq.*

[24] 15 U.S.C. § 6802(e).

business to carry out the activity covered by the exception under which ... the information [was received]."[25]

C. Limiting the Use and Disclosure of SSNs

As described above, the SSN is valuable in enabling entities to match information to consumers. With 300 million Americans, many of whom share the same name, the SSN presents significant advantages as a means of identification because of its uniqueness and permanence. The misuse of SSNs, however, can facilitate identity theft. The challenge is to find the proper balance between the necessity of keeping SSNs out of the hands of identity thieves, while giving businesses and government sufficient means to match information to the correct person. Excessive restrictions on the use of SSNs could have a deleterious impact on such important purposes as public health, criminal law enforcement, and anti-fraud and anti-terrorism efforts.

SSNs are available to identity thieves, in part, because they are widely used as consumer identifiers, i.e., to associate information with particular individuals. For example, SSNs sometimes are used as identification numbers displayed on identification cards. These SSNs are extremely valuable to identity thieves. They frequently are used by creditors and other benefit providers to access information (such as a credit report) that is necessary to open an account or provide other benefits. Unless the creditor obtains sufficient additional authenticating information - i.e., information proving that the individual is who he purports to be - a thief with a consumer's name and SSN, and perhaps additional information or documentation, may be able to open an account by impersonating the consumer. In short, the SSN is both widely available and valuable to identity thieves.

---

[25] 16 C.F.R. Part 313.11(a).

Preventing the misuse of SSNs, therefore, can follow two paths. First, the unnecessary use and disclosure of SSN as an identifier can be reduced. The Identity Theft Task Force is working toward this goal. For example, one of its interim recommendations was that the federal government review its collection and use of SSNs with the goal of eliminating them wherever possible.

Second, to prevent misuse of SSNs, improved methods of authenticating consumers can be promoted so that, even if the SSN falls into the hands of an identity thief, that SSN is less valuable. On April 23 and 24, 2007, the Commission will sponsor a workshop on authentication. The workshop is designed to facilitate discussions among knowledgeable parties about the technological and policy issues surrounding the development of improved authentication procedures.[26]

V. CONCLUSION

Identity theft remains a serious problem in our economy, causing enormous harm to consumers and businesses and threatening consumer confidence in the marketplace. To succeed in the battle against identity theft, government and the private sector, working together, must make it more difficult for thieves to obtain the information they need to steal identities, and make it more difficult to use that information if they obtain it. There are several actions that should be taken to further these goals. To prevent thieves from obtaining sensitive information, government and the business community must better protect their data, and must consider what information they collect and maintain from or about consumers and whether they need to do so.

---

[26] *See Proof Positive: New Directions for ID Authentication*, 72 Fed. Reg. 8381 (Feb. 26, 2007); http://www.ftc.gov/bcp/workshops/proofpositive/index.html.

In this regard, eliminating unnecessary collection, use, and disclosure of Social Security numbers - an important tool of identity thieves - can play a key role. To keep thieves from using the information they do procure to steal identities, better means of consumer authentication must be developed and implemented. The Commission will continue and strengthen its law enforcement efforts, as well as its education and outreach to guide and empower businesses and consumers to fight back against identity theft.